Finite algebras of relations are representable on finite sets

H. Andréka, I. Hodkinson, I. Németi*

13 December 1996

Abstract

Using a combinatorial theorem of Herwig on extending partial isomorphisms of relational structures, we give a simple proof that certain classes of algebras, including Crs, polyadic Crs, and WA, have the 'finite base property' and have decidable universal theories, and that any finite algebra in each class is representable on a finite set.

1 Introduction

In this paper, we give a simple proof that certain classes K of algebras have the 'finite base property'. This will imply decidability of the universal theory of K, and that any finite algebra in K is representable on a finite set. Examples of such K include the relativized cylindric set algebras in dimension n (Crs_n), polyadic Crs, and the weakly associative relation algebras WA. Most of these results were first established in the paper [ABN2]; the original proofs were substantially longer than the present one.

What is the finite base property?

Say that we are given a class K of concrete algebras. This is to say that the algebras in K have the form $\mathcal{A} = \langle A, f, g, \ldots \rangle$, where A is the domain of $\mathcal{A}$, and $f, g, \ldots$ are functions defined on A. However, the domain A is not merely an abstract set, but has intrinsic structure; and $f, g, \ldots$ are defined in terms of this structure, uniformly over K. In fact, A will typically be a subset of $\wp(W)$, the power set of some set W of sequences of elements of another set, U. All the sequences will have the same finite length, n, so in symbols we have $W \subseteq {}^nU$. The definitions of the functions f, g then utilise the form of the elements of A as sets of sequences. For example, for $a, b \in A$, $f(a, b)$ might be $a \cap b$, while $g(a)$ might be the set of reverses of the sequences in a (the reverse of $\langle s_0, \ldots, s_{n-1} \rangle$ being $\langle s_{n-1}, \ldots, s_0 \rangle$), and so on.

*Andréka and Németi were supported by the Hungarian National Foundation for Scientific Research, grant numbers T16448, T7255. We thank Szabolcs Mikulás for helpful comments on drafts of this paper.

The sets W and U associated with $\mathcal{A}$ are not unique — any larger sets will do too — but there will be unique *smallest* such sets for each $\mathcal{A}$. The smallest W, obtainable as the union of all elements of $\mathcal{A}$, is called the *unit* of $\mathcal{A}$. The smallest U, obtainable as the set of all elements occurring in sequences in the unit, is called the *base* of $\mathcal{A}$.

The class K is now said to have the *finite base property* if any universal sentence in the signature of K that is not valid in K is not valid in some $\mathcal{A} \in \mathsf{K}$ with finite base. This property implies that a finite algebra (in finite similarity type) is isomorphic to one with a finite base (by taking the negation of the diagram of the algebra as our universal sentence: see the proof of theorem 4). It is formally stronger than what we may call the 'finite algebra property', which says that a non-valid universal sentence may be falsified in some finite $\mathcal{A} \in \mathsf{K}$ (i.e., with finite domain). An algebra in K could be finite and yet have infinite base.

Why is the finite base property of interest? For one thing, it suggests that K is in some way a 'nice' class. For example, the algebras in K with finite base can often be enumerated recursively — certainly, this is true for the classes K we consider here. So if the universal theory Σ of K is recursively axiomatisable, the finite base property implies decidability of Σ. (In fact, we will show that there is a recursive bound on the size of the base of the algebra witnessing non-validity of a universal sentence ϕ, in terms of the syntactic size of ϕ. This yields decidability of Σ whether or not Σ is known to be recursively axiomatisable.) Notice that the finite algebra property is not sufficient in this regard, for as a finite algebra can have infinite base, it is not clear that we can recursively enumerate all finite algebras in K. For more information see [N92].

Further, given $\mathcal{A} = \langle \wp(W), f, g, \ldots \rangle \in \mathsf{K}$, we may view W in a modal-logical way. We consider the modal formulas formed using a (k-ary) connective $\sharp_f$ for each (k-ary) function f of $\mathcal{A}$. We evaluate them at sequences in W — so W is the set of possible worlds of our model. The intended semantics is that if (inductively) the sets of sequences in W at which formulas $\varphi_1, \ldots, \varphi_k$ hold are $a_1, \ldots, a_k$, respectively, then the formula $\sharp_f(\varphi_1, \ldots, \varphi_k)$ will hold precisely at the sequences in $f(a_1, \ldots, a_k)$. If f happens to be 'normal and completely additive' (in the current context, this means $f(a_1, \ldots, a_k) = \bigcup_{s_i \in a_i, i \leq k} f(\{s_1\}, \ldots, \{s_k\})$ for all $a_1, \ldots, a_k \subseteq W$), the connective $\sharp_f$ has a genuinely modal (Kripke) semantics, via the $(k+1)$-ary accessibility relation R_f defined in the following standard way: for all $s_0, \ldots, s_k \in W$, $R_f(s_0, \ldots, s_k)$ holds iff $s_0 \in f(\{s_1\}, \ldots, \{s_k\})$. This justifies our calling the logic 'modal', as many of the functions usually considered (including those in this paper) are indeed normal and completely additive. The exceptions are the boolean operations (for example, $W \vee \emptyset = W$, while $\bigcup_{s_1 \in W, s_2 \in \emptyset} s_1 \vee s_2 = \emptyset$) and, here, the counting quantifiers.

In this setting the modal formulas will correspond to algebraic terms, and validity of *formulas* in W to validity of *equations* in $\mathcal{A}$. So the logic is decidable iff the equational theory of K is. The finite base property *for equations only* now corresponds to a strong n-dimensional form of the modal finite model property familiar to modal logicians.

Modalizing the classes of algebras studied here yields variants of the n-variable fragment of first-order logic, with semantics differing from the classical Tarskian view because W need not be of the form ${}^nU$. These 'mutant' logics are under intensive study at the present time, and we cite [ABN1, VM] as sources. They frequently have desirable properties that n-variable first-order logic lacks (such as decidability, Craig interpolation, Beth definability).

The finite base property can also be useful in obtaining other theorems. For example: by the finite base property for cylindric-relativized set algebras (Crs_n), any finite Crs_n can be obtained by relativizing a finite cylindric set algebra (Cs_n). This was used by A. Simon [S] to prove that every finite cylindric algebra of dimension 3 can be obtained by twisting and relativization from a finite Cs_3. The finite base property for our classes K also can be seen as a combinatorial principle that we formalize roughly as 'any finite pattern of n-ary relations can be realized also with finite n-ary relations'.

We will prove the finite base property for several classes of algebras, including the classes Crs, polyadic Crs, WA, and locally cubic n-dimensional relativized cylindric set algebras augmented with substitution operators. For definitions of these see section 3 and example 22, or [HMT,Madd]; but they all fit the framework described above, varying only in what functions are present and what properties of W are assumed. We actually prove a single result (theorem 4) that gives most of these as corollaries, and then extend it (theorem 23) to give the rest.

The proof of theorem 4 starts off similarly to modal filtration, which is entirely natural, as the finite base property is analogous to the modal finite model property. However, this does not necessarily yield an algebra whose elements are sets of sequences and with the functions defined in terms of this internal structure. So our proof must involve more work. The chief extra argument used is the following combinatorial theorem of Herwig. Theorem 23 is proved similarly, using a stronger version (theorem 16 below, from [He2]), and it establishes the finite base property for further classes of algebras, including the weakly associative algebras — a new result, we believe.

THEOREM 1 (HERWIG, [HE1]) *Let $\mathfrak{K}$ be a finite structure in a finite relational language L. There is a finite L-structure $\mathfrak{K}^+ \supseteq \mathfrak{K}$ such that any partial isomorphism of $\mathfrak{K}$ is induced by an automorphism of $\mathfrak{K}^+$.*

Herwig's proof generalizes arguments of Hrushovski [Hr]. A primitive recursive upper bound on the cardinality $|\mathfrak{K}^+|$ of the domain of $\mathfrak{K}^+$ in terms of $k = |\mathfrak{K}|$ and L may be extracted from the proof. The existence of a recursive bound follows from the theorem itself, as for each of the finitely many L-structures $\mathfrak{K}$ with domain of size k, we may enumerate all finite L-structures extending $\mathfrak{K}$, stopping when we find one with the property of the theorem. Lascar has a simpler proof of theorem 1, which may give a better bound. This will appear in a joint paper with Herwig, which places the result in the setting of free groups.

We will also borrow an idea from [MM] when dealing with counting quantifiers.

The ideas presented here will also yield a completeness theorem for the associated modal logic, without using 'step-by-step' arguments — see [VM,HHMMR].

The layout of the paper is as follows. In section 2 we prove the finite base property for a fairly general class of algebras, and in section 3 we use this result and the notion of subreducts to get the property for more classes. In section 4 we extend the results of section 2 to classes such as WA. In the final section we discuss some of the implications of these results.

Notation

Our notation is mostly standard, but the following list may help.

Sets. If X is a set, $|X|$ denotes the cardinality of X, and $\wp X$ the set of all subsets (the power set) of X. Id_X is the identity map on X. The ordinal $n < \omega$ is identified with $\{0, 1, \ldots, n-1\}$. If $\theta : X \to Y$ is a map, and $X' \subseteq X$, we write $\theta\lceil X'$ for the restriction of θ to X'.

Sequences. Let X be a set, and $n < \omega$. An (n-)sequence (or n-tuple) of elements of X is a map from n into X. The set of all such sequences is denoted by ${}^nX$. We use $s, t, \ldots$ to denote sequences of elements, and $\bar{x}, \bar{y}$ to denote sequences (or tuples) of variables. The length of $\bar{x}$ is denoted by $\text{len}(\bar{x})$. For $i < n$, the ith element of a sequence s is written as s_i, and we can write s as $\langle s_0, \ldots, s_{n-1}\rangle$. If $\sigma : n \to n$, then $s \circ \sigma$ is just the composition of the maps σ, s: so $(s \circ \sigma)_i = s_{\sigma(i)}$ for each $i < n$. If $\alpha : X \to Y$ and $s \in {}^nX$, then $s\alpha$ denotes the sequence $\langle s_0\alpha, \ldots, s_{n-1}\alpha\rangle \in {}^nY$. (Maps are often written on the right.) Thus $s \circ \sigma$ is the sequence 'rearranged' according to σ, while $s\alpha$ is the sequence where the 'letters' occurring in s are replaced according to α.

If $\Gamma = \{i_0, \ldots, i_{k-1}\} \subseteq n$, where $i_0 < \cdots < i_{k-1}$, then for $s \in {}^nX$, $s\lceil\Gamma$ denotes the sequence $\langle s_{i_0}, \ldots, s_{i_{k-1}}\rangle \in {}^kX$. $s \equiv_\Gamma t$ will mean that $s\lceil(n \setminus \Gamma) = t\lceil(n \setminus \Gamma)$, or equivalently, $s_i = t_i$ for all $i \in n \setminus \Gamma$.

$\text{Rng}(s)$ denotes the range of s: i.e., $\text{Rng}(s) = \{s_i : i < n\}$. The concatenation st of sequences $s \in {}^nX, t \in {}^mX$ is the sequence $u \in {}^{n+m}X$ given by

$$u_i = \begin{cases} s_i, & \text{if } i < n \\ t_{i-n}, & \text{if } n \leq i < n+m. \end{cases}$$

Model theory. Classical model-theoretic (first-order) structures will be denoted by gothic letters. The domain (or universe) of the structure $\mathfrak{K}$ will be written as K; it is always non-empty. A relational signature (or similarity type) is one with no function symbols or constants. Apart from algebras (below), we will only consider relational structures (structures in a relational signature), or at worst structures whose signature L has no function symbols except possibly constants. If $\mathfrak{K}$ is an L-structure and R is an m-ary relation symbol in L, we write $R^{\mathfrak{K}}$ for the interpretation of R in $\mathfrak{K}$. So $R^{\mathfrak{K}} \subseteq {}^mK$. An L-structure $\mathfrak{J}$ is said to be a substructure of $\mathfrak{K}$ — in symbols, $\mathfrak{J} \subseteq \mathfrak{K}$ — if $J \subseteq K$ and $\mathfrak{J} \models R(s)$ iff $\mathfrak{K} \models R(s)$ for each $R \in L$ (m-ary) and $s \in {}^mJ$. If $X \subseteq K$, $\mathfrak{K}\lceil X$ denotes the substructure of $\mathfrak{K}$ with domain X. We say that L-structures $\mathfrak{J}, \mathfrak{K}$ are isomorphic (written $\mathfrak{J} \cong \mathfrak{K}$) if there is a bijection between their domains that preserves all atomic L-formulas in both directions.

A partial isomorphism of $\mathfrak{K}$ is a partial one-to-one map α on K such that for each atomic L-formula $\varphi(x_0, \ldots, x_{m-1})$ and $s \in {}^m(dom(\alpha))$, $\mathfrak{K} \models \varphi(s) \leftrightarrow \varphi(s\alpha)$. Note that partial isomorphisms will be written as acting on the right. An automorphism of $\mathfrak{K}$ is a partial isomorphism of $\mathfrak{K}$ that is a permutation of K (a bijection : $K \to K$). The set $Aut(\mathfrak{K})$ of all automorphisms of $\mathfrak{K}$ forms a group under composition and inverse of permutations, with identity element Id_K.

Algebras. These are structures whose signature has no relation symbols, but only function symbols and constants. They play a different role from the classical structures here, so we will write them differently, as $\mathcal{A}, \mathcal{B}, \ldots$, with domains $A, B, \ldots$. Note that the domain of an algebra may have pertinent intrinsic structure, as we saw. If u is an assignment of variables to elements of the domain of $\mathcal{A}$, we write $\tau^{(\mathcal{A},u)}$ for the value of the term τ in $\mathcal{A}$ under this assignment. So $\tau^{(\mathcal{A},u)} \in A$. If τ has no variables, we may write $\tau^{\mathcal{A}}$ instead. In the same way, if f is a function symbol of the signature of $\mathcal{A}$, we write $f^{\mathcal{A}}$ for its interpretation in $\mathcal{A}$ as a function on A. For terms τ, σ, we write $\mathcal{A} \models \tau = \sigma[u]$ if $\tau^{(\mathcal{A},u)} = \sigma^{(\mathcal{A},u)}$.

Up to isomorphism there is a unique algebra in any signature with domain of size 1.

Conventions. n will be the algebra dimension; i, j will denote ordinals $< n$; σ will denote a map : $n \to n$; and Γ will denote a subset of n.

2 Proving the finite base property

We wish to prove the finite base property for various classes of algebras, which are defined in section 3 below. Rather than prove many similar theorems, we will show that the following class C of algebras has the finite base property, and then derive the particular results as corollaries using the notion of *subreducts* (definition 9). Some classes (such as WA) that do not succumb to this will be dealt with later, in theorem 23.

Recall that n, the dimension, is fixed throughout and satisfies $2 \leq n < \omega$.

2.1 Definitions

DEFINITION 2 Define C to be the class of all algebras $\mathcal{A}$ of the following form. The signature or vocabulary of $\mathcal{A}$ consists of the following function symbols:

binary: $\cdot$ (used in infix form)

unary: $-$, $\mathsf{c}_{(\Gamma)}$, s_σ, and e_r, for each $\Gamma \subseteq n$, $\sigma : n \to n$, $r < \omega$. We may write c_i instead of $\mathsf{c}_{(\{i\})}$, for $i < n$.

constant symbols: $0, 1$, and d_{ij}, for each $i, j < n$.

The domain or universe of $\mathcal{A}$ is a subset A of $\wp(W)$, where $W \subseteq {}^nU$ for some arbitrary set U. It is mandatory that A contains the interpretations of the constant symbols and is closed under the interpretations of the function symbols. These are:

- '$\cdot$' is interpreted as intersection, and '$-$' as complement relative to W (that is, $a \cdot b = a \cap b$ and $-a = W \setminus a$, for all $a, b \in A$).
- 0 and 1 are interpreted as $\emptyset$ and W, respectively. W is called the *unit* of the algebra.
- d_{ij} is interpreted as the 'diagonal' $\{s \in W : s_i = s_j\}$.
- s_σ is interpreted as substitution via the map σ: for each $a \in A$, $\mathsf{s}_\sigma^{\mathcal{A}} a = \{s \in W : s \circ \sigma \in a\}$.
- $\mathsf{c}_{(\Gamma)}$ is interpreted as cylindrification along all components in Γ: for each $a \in A$, $\mathsf{c}_{(\Gamma)}^{\mathcal{A}} a = \{s \in W : s \equiv_\Gamma t \text{ for some } t \in a\}$.
- e_r is a counting quantifier. For each $r < \omega$, $\mathsf{e}_r a$ is interpreted as W if $|a| \geq r$, and $\emptyset$ otherwise, for each $a \in A$. That is, $\mathsf{e}_r^{\mathcal{A}} a = \{s \in W : |a| \geq r\}$. The e_r are sometimes called 'graded modalities'.

See the previous section for notation used here. Thus, $\mathcal{A}$ has the form

$$\langle A, \cdot, -, 0, 1, \mathsf{d}_{ij}, \mathsf{s}_\sigma, \mathsf{c}_{(\Gamma)}, \mathsf{e}_r \rangle_{i,j<n,\, \sigma:n\to n,\, \Gamma\subseteq n,\, r<\omega}.$$

DEFINITION 3 The *base* of an algebra $\mathcal{A} \in \mathsf{C}$ is the smallest set U such that $1^{\mathcal{A}} \subseteq {}^n U$.

2.2 Finite base property for C

THEOREM 4 *Any universal sentence that is not valid in C is falsifiable in an algebra $\mathcal{A} \in \mathsf{C}$ with finite base. In fact, from the universal sentence we can compute an upper bound for the size of this finite base.*

Hence, the universal theory of C is decidable; and if C' is the class of reducts of algebras in C to any finite signature, then any finite algebra in C' is isomorphic to an algebra in C' with finite base.

PROOF.

Let $\mathcal{T}$ be any finite set of terms in the language of C that is closed under taking subterms, let $\mathcal{A} \in \mathsf{C}$, and let u be an assignment of the variables in $\mathcal{T}$ to elements of $\mathcal{A}$. We will construct an algebra $\mathcal{B} \in \mathsf{C}$ with finite base and an assignment v of the same variables to elements of $\mathcal{B}$ such that for all $\tau, \sigma \in \mathcal{T}$,

$$(*) \qquad \mathcal{A} \models \tau = \sigma[u] \quad \text{iff} \quad \mathcal{B} \models \tau = \sigma[v].$$

This will imply the first part of theorem 4 because of the following. Let $\forall \bar{x} \psi$ be a universal sentence that is not valid in C, where ψ is quantifier-free. Let $\mathcal{T}$ be the set of terms occurring in ψ, and let $\mathcal{A} \in \mathsf{C}$ and u be such that $\mathcal{A} \not\models \psi[u]$. Take $\mathcal{B} \in \mathsf{C}$ with finite base and v for which $(*)$ holds. Then clearly, $\mathcal{B} \not\models \psi[v]$, and so $\forall \bar{x} \psi$ fails in a member of C with finite base.

So let $\mathcal{T}, \mathcal{A}$ and u as above be given. We may assume that $1 \in \mathcal{T}$. Let the base of $\mathcal{A}$ be U, and let Q be an arbitrary finite subset of U. (We will use Q to handle the counting operations e_r; in this we borrow an idea from [MM]. So at the moment Q is arbitrary, but later we will make a restriction on it.)

Form a first-order relational signature $\overline{\mathcal{T}}$ as follows. For each term $\tau \in \mathcal{T}$, $\overline{\mathcal{T}}$ contains a relation symbol $\overline{\tau}$. If τ does not begin with $\mathsf{c}_{(\Gamma)}$ for some Γ, then the arity of $\overline{\tau}$ is n. Otherwise, τ begins with $\mathsf{c}_{(\Gamma)}$, so is of form $\mathsf{c}_{(\Gamma)}\tau'$ for some τ', and in this case the arity of $\overline{\tau}$ is $n - |\Gamma|$. (This is so even if τ' is itself of the form $\mathsf{c}_{\Delta}\tau''$.)

Now create a classical first-order $\overline{\mathcal{T}}$-structure $\mathfrak{U}$ as follows. The domain of $\mathfrak{U}$ is U. The relation symbol $\overline{\tau}$ is interpreted in $\mathfrak{U}$ as $\tau^{(\mathcal{A},u)}$ if the arity of $\overline{\tau}$ is n. Otherwise, τ is of the form $\mathsf{c}_{(\Gamma)}\tau'$, and then we interpret $\overline{\tau}$ in $\mathfrak{U}$ as $\{s\lceil(n \setminus \Gamma) : s \in \tau'^{(\mathcal{A},u)}\}$. For example, if $\Gamma = n$ then $\overline{\tau}^{\mathfrak{U}}$ is either the set containing the empty tuple, if $\tau'^{(\mathcal{A},u)} \neq \emptyset$, or the empty set, otherwise. (Notice that we define $\overline{\tau}^{\mathfrak{U}}$ in terms of $\tau'^{(\mathcal{A},u)}$, and not $\overline{\tau'}^{\mathfrak{U}}$, which may have lower arity than n.)

For any $s \in {}^nU$ we define the structure $\mathfrak{U}(s)$ to be the finite substructure of $\mathfrak{U}$ with domain $Q \cup \mathrm{Rng}(s)$, expanded by additional constants naming $s_0, \ldots, s_{n-1}$ and the elements of Q. More precisely, we introduce new constants $\mathbf{a}_q$ and $\mathbf{a}_i$ for each $q \in Q$ and $i < n$. (We may assume that $Q \cap n = \emptyset$.) The signature of each $\mathfrak{U}(s)$ is always the same, namely $\overline{\mathcal{T}} \cup \{\mathbf{a}_q, \mathbf{a}_i : q \in Q, i < n\}$. In $\mathfrak{U}(s)$, the interpretation of $\mathbf{a}_q$ is q, and the interpretation of $\mathbf{a}_i$ is s_i, for each $q \in Q$ and $i < n$, while with regard to relation symbols in $\overline{\mathcal{T}}$, $\mathfrak{U}(s)$ is a substructure of $\mathfrak{U}$.

LEMMA 5 *If $s, t \in {}^nU$ and $\mathfrak{U}(s) \cong \mathfrak{U}(t)$, then $s \in \tau^{(\mathcal{A},u)}$ iff $t \in \tau^{(\mathcal{A},u)}$ for all $\tau \in \mathcal{T}$.*

PROOF.

Indeed, assume that $\mathfrak{U}(s) \cong \mathfrak{U}(t)$. The unique isomorphism between $\mathfrak{U}(s)$ and $\mathfrak{U}(t)$ takes s to t. First let $\tau \in \mathcal{T}$ be any term which does not begin with any $\mathsf{c}_{(\Gamma)}$. Then $s \in \tau^{(\mathcal{A},u)}$ iff $\mathfrak{U}(s) \models \overline{\tau}(s)$ iff $\mathfrak{U}(t) \models \overline{\tau}(t)$ iff $t \in \tau^{(\mathcal{A},u)}$. In particular, $s \in 1^{\mathcal{A}}$ iff $t \in 1^{\mathcal{A}}$, since $1 \in \mathcal{T}$.

Assume now that τ is of form $\mathsf{c}_{(\Gamma)}\tau'$. If $s \notin 1^{\mathcal{A}}$, then as $t \notin 1^{\mathcal{A}}$ too, $s, t \notin \tau^{(\mathcal{A},u)}$. So we may assume that $s, t \in 1^{\mathcal{A}}$. Then

$$(\dagger) \qquad s \in \tau^{(\mathcal{A},u)} \quad \text{iff} \quad \mathfrak{U}(s) \models \overline{\tau}(s\lceil(n \setminus \Gamma)),$$

and the same for t, because of the following. By the definition of $\overline{\tau}^{\mathfrak{U}(s)}$ we have that $\mathfrak{U}(s) \models \overline{\tau}(s\lceil(n \setminus \Gamma))$ iff there is $z \in \tau'^{(\mathcal{A},u)}$ such that $s \equiv_{\Gamma} z$, which by $s \in 1^{\mathcal{A}}$ holds iff $s \in \mathsf{c}^{\mathcal{A}}_{(\Gamma)}\tau'^{(\mathcal{A},u)} = \tau^{(\mathcal{A},u)}$.

Now $(\dagger)$ together with $\mathfrak{U}(s) \cong \mathfrak{U}(t)$ implies that $s \in \tau^{(\mathcal{A},u)}$ iff $t \in \tau^{(\mathcal{A},u)}$, as required. ♣

The structures $\mathfrak{U}(s)$ ($s \in {}^nU$) have at most $|Q| + n$ elements and their language is finite, so that there are only finitely many isomorphism types of them. Choose a finite subset $K \subseteq U$ such that for all $s \in {}^nU$ there is $t \in {}^nK$ with $\mathfrak{U}(t) \cong \mathfrak{U}(s)$. Necessarily, $Q \subseteq K$ (though of course, if this were not true we could simply add Q to K). For, if $q \in Q$, then $q \in U$, so there are $s \in 1^{\mathcal{A}}$ and $j < n$ with $s_j = q$. Let $t \in {}^nK$ with $\mathfrak{U}(t) \cong \mathfrak{U}(s)$. Then $t_j = q$ since by $s_j = q$ we have that $\mathfrak{U}(s) \models \mathbf{a}_j = \mathbf{a}_q$, so the same holds in $\mathfrak{U}(t)$. Then $q \in K$ by $t \in {}^nK$.

Let $\mathfrak{K}$ be the substructure of $\mathfrak{U}$ with domain K. It has a finite relational signature, so we may use Herwig's theorem (theorem 1) to obtain a finite $\overline{\mathcal{T}}$-structure $\mathfrak{K}^+ \supseteq \mathfrak{K}$ such that any partial isomorphism of $\mathfrak{K}$ is induced by an automorphism of $\mathfrak{K}^+$. Let G be the group consisting of all automorphisms of $\mathfrak{K}^+$ that fix Q pointwise — that is,

$$G = \{g \in Aut(\mathfrak{K}^+) : xg = x \text{ for all } x \in Q\}.$$

Let

$$H = \{sg : s \in \overline{1}^{\mathfrak{K}},\, g \in G\} \subseteq {}^nK^+.$$

We now obtain an algebra

$$\mathcal{B} = \langle \wp(H), \cdot, -, \emptyset, H, \mathsf{d}_{ij}, \mathsf{s}_\sigma, \mathsf{c}_{(\Gamma)}, \mathsf{e}_r \rangle_{i,j<n,\, \sigma:n\to n,\, \Gamma\subseteq n,\, r<\omega} \quad \in \mathsf{C}.$$

The base of $\mathcal{B}$ is a subset of K^+, and so is finite.

Define an assignment v of the variables in $\mathcal{T}$ to elements of the domain of $\mathcal{B}$, by: $v(y) = \{s \in H : \mathfrak{K}^+ \models \overline{y}(s)\}$.

LEMMA 6 *For any $g \in G$, $\tau \in \mathcal{T}$, and $s \in \tau^{(\mathcal{B},v)}$, we have $sg \in \tau^{(\mathcal{B},v)}$ also.*

PROOF.

A simple induction on τ. We want to prove that $\tau^{(\mathcal{B},v)}$ is preserved by G. Note that $1^{\mathcal{B}} = H$ is preserved under G since G is a group (closed under multiplication). Also, $y^{(\mathcal{B},v)} = v(y)$ is preserved by G, since each element of G is an automorphism of $\mathfrak{K}^+$ and H is preserved under G. The rest follows from the fact that each operation of $\mathcal{B}$ is permutation-invariant, so if all the arguments are preserved by G then the result of the operation is also preserved by G. ♣

We can now prove the main lemma, analogous to the 'truth lemma' in modal filtration.

LEMMA 7 *For all $\tau \in \mathcal{T}$, we have $s \in \tau^{(\mathcal{A},u)}$ iff $s \in \tau^{(\mathcal{B},v)}$ for every $s \in {}^nK$.*

PROOF.

By induction on the structure of τ. Let $s \in {}^nK$ be arbitrary.

The case $\tau = 0$. Trivial.

The case $\tau = 1$. Then $s \in 1^{\mathcal{B}}$ iff $s \in H$, iff $sg \in {}^nK$ and $\mathfrak{K} \models \overline{1}(sg)$ for some $g \in G$, iff $sg \in {}^nK$ and $\mathfrak{K}^+ \models \overline{1}(sg)$ for some $g \in G$ (because $\mathfrak{K} \subseteq \mathfrak{K}^+$). This holds iff $\mathfrak{K}^+ \models \overline{1}(s)$ — '$\Rightarrow$' because $G \subseteq Aut(\mathfrak{K}^+)$, and '$\Leftarrow$' because $s \in {}^nK$ already. This is equivalent to $\mathfrak{K} \models \overline{1}(s)$ (since $s \in {}^nK$ and $\mathfrak{K} \subseteq \mathfrak{K}^+$), i.e., to $s \in 1^{\mathcal{A}}$, by definition of $\mathfrak{K}$.

The case where τ is a variable. We have $s \in v(\tau)$ iff $s \in H = 1^{\mathcal{B}}$ and $\mathfrak{K}^+ \models \overline{\tau}(s)$. By the preceding case, $\tau = 1$, and the fact that $\mathfrak{K} \subseteq \mathfrak{K}^+$, this is iff $s \in 1^{\mathcal{A}}$ and $\mathfrak{K} \models \overline{\tau}(s)$, which holds iff $s \in 1^{\mathcal{A}}$ and $s \in u(\tau)$, by definition of $\mathfrak{K}$. This is iff $s \in u(\tau)$, as required.

The case $\tau = \mathsf{d}_{ij}$. Clear, since $s \in \mathsf{d}_{ij}^{\mathcal{A}}$ iff $s \in 1^{\mathcal{A}}$ and $s_i = s_j$, iff $s \in 1^{\mathcal{B}}$ and $s_i = s_j$ (by the case $\tau = 1$ above), iff $s \in \mathsf{d}_{ij}^{\mathcal{B}}$.

The case $-\tau$. Assume the lemma for τ. We have $s \in -\tau^{(\mathcal{A},u)}$ iff $s \in 1^{\mathcal{A}}$ and $s \notin \tau^{(\mathcal{A},u)}$, iff $s \in 1^{\mathcal{B}}$ and $s \notin \tau^{(\mathcal{B},v)}$ (by the case $\tau = 1$ and the inductive hypothesis), iff $s \in -\tau^{(\mathcal{B},v)}$.

The case $\tau \cdot \tau'$. The proof is obvious.

The case $\mathsf{s}_\sigma \tau$. Assume the lemma for τ. Then $s \in (\mathsf{s}_\sigma \tau)^{(\mathcal{A},u)}$ iff $s \in 1^{\mathcal{A}}$ and $s \circ \sigma \in \tau^{(\mathcal{A},u)}$. Note that $s \circ \sigma \in {}^nK$, also. So by the case $\tau = 1$ and the inductive hypothesis, this is equivalent to $s \in 1^{\mathcal{B}}$ and $s \circ \sigma \in \tau^{(\mathcal{B},v)}$, i.e., $s \in (\mathsf{s}_\sigma \tau)^{(\mathcal{B},v)}$.

The case $\mathsf{c}_{(\Gamma)}\tau$. This is where the real work starts. Assume the lemma for τ. Suppose first that $s \in (\mathsf{c}_{(\Gamma)}\tau)^{(\mathcal{B},v)}$. Then there is $t \in \tau^{(\mathcal{B},v)}$ with $t \equiv_\Gamma s$. Choose $g \in G$ such that $tg \in {}^nK$; g exists because $t \in \tau^{(\mathcal{B},v)} \subseteq 1^{\mathcal{B}} = H$. Now by lemma 6, $tg \in \tau^{(\mathcal{B},v)}$ also; by the inductive hypothesis, $tg \in \tau^{(\mathcal{A},u)}$. So certainly, $tg \in (\mathsf{c}_{(\Gamma)}\tau)^{(\mathcal{A},u)}$. By definition of $\mathfrak{K}$, it follows that $\mathfrak{K} \models \overline{\mathsf{c}_{(\Gamma)}\tau}(tg\lceil(n \setminus \Gamma))$. As g^{-1} is an automorphism of $\mathfrak{K}^+$, of which $\mathfrak{K}$ is a substructure, and $t\lceil(n \setminus \Gamma) = s\lceil(n \setminus \Gamma) \in {}^{n-|\Gamma|}K$, we can apply g^{-1} to this and get $\mathfrak{K} \models \overline{\mathsf{c}_{(\Gamma)}\tau}(s\lceil(n \setminus \Gamma))$. So by definition of $\mathfrak{K}$, there is $s' \in \tau^{(\mathcal{A},u)}$ with $s' \equiv_\Gamma s$. Hence, $s \in (\mathsf{c}_{(\Gamma)}\tau)^{(\mathcal{A},u)}$. Note that for this last step we need to know that $s \in 1^{\mathcal{A}}$; but $s \in (\mathsf{c}_{(\Gamma)}\tau)^{(\mathcal{B},v)} \subseteq 1^{\mathcal{B}}$, so by the case $\tau = 1$, $s \in 1^{\mathcal{A}}$. See figure 1.

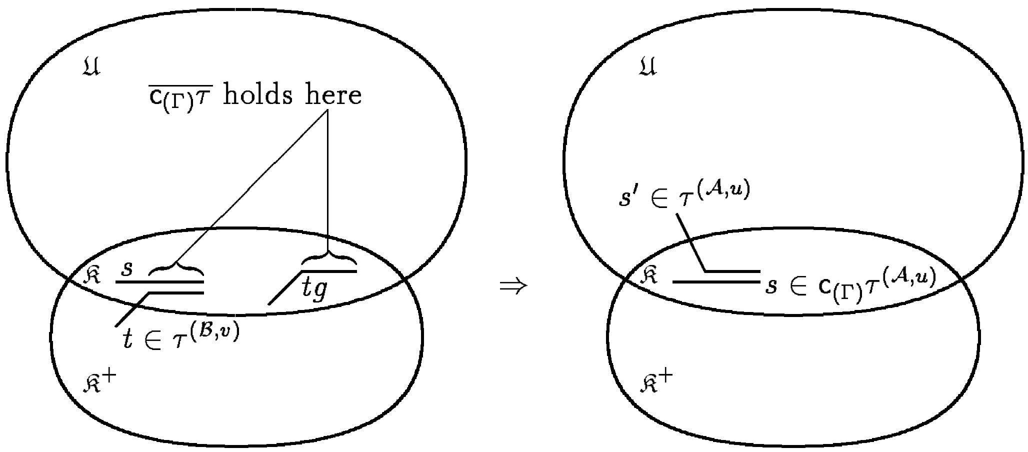

FIGURE 1.

Conversely, assume that $s \in (\mathsf{c}_{(\Gamma)}\tau)^{(\mathcal{A},u)}$. So there is $t \in \tau^{(\mathcal{A},u)}$ with $t \equiv_\Gamma s$. We may not have $t \in {}^nK$, but by choice of K there does exist $t' \in {}^nK$ with $\mathfrak{A}(t') \cong \mathfrak{A}(t)$. Let $\alpha : \mathfrak{A}(t') \to \mathfrak{A}(t)$ be the unique isomorphism. Then as $t_i = s_i$ for all $i \in n \setminus \Gamma$, the domain and range of the map

$$\beta \;=\; \alpha\lceil(Q \cup \{t'_i : i \in n \setminus \Gamma\})$$

are contained in K, so β is a partial isomorphism of $\mathfrak{K}$.
Using the properties of $\mathfrak{K}^+$ given by Herwig's theorem, let g be an automorphism of $\mathfrak{K}^+$ extending β. Now by lemma 5, $t' \in \tau^{(\mathcal{A},u)}$, so by the inductive hypothesis, $t' \in \tau^{(\mathcal{B},v)}$. Clearly, $g \in G$, so by lemma 6, $t'g \in \tau^{(\mathcal{B},v)}$. But $t'g \equiv_\Gamma t \equiv_\Gamma s$. As $s \in 1^{\mathcal{B}}$ (by reversing the proof that $s \in 1^{\mathcal{A}}$, above), we obtain $s \in (\mathsf{c}_{(\Gamma)}\tau)^{(\mathcal{B},v)}$, as required. See figure 2.

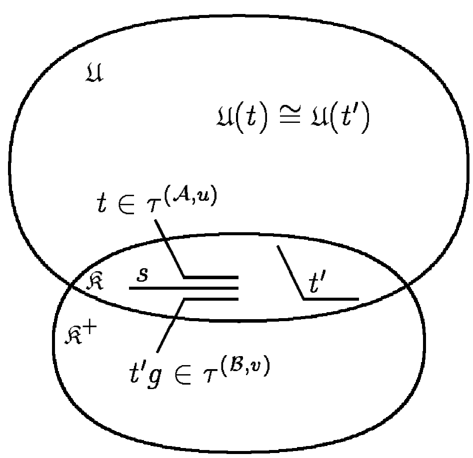

FIGURE 2.

The case $\mathsf{e}_r\tau$. Recall that Q has so far been an arbitrary finite subset of U, the base of $\mathcal{A}$. We now require that it is large enough to ensure that for each term in $\mathcal{T}$ of the form $\mathsf{e}_r\tau$,

$$(**) \qquad |\tau^{(\mathcal{A},u)} \cap {}^nQ| \geq \min(|\tau^{(\mathcal{A},u)}|, r).$$

This is easily arranged. Now let $\mathsf{e}_r\tau \in \mathcal{T}$ and assume the lemma for τ.

Claim. $|\tau^{(\mathcal{A},u)}| \geq r \iff |\tau^{(\mathcal{B},v)}| \geq r$.
Proof of claim. Assume that $|\tau^{(\mathcal{A},u)}| \geq r$. It follows from $(**)$ that $|\tau^{(\mathcal{A},u)} \cap {}^nQ| \geq r$. Since inductively, $\tau^{(\mathcal{A},u)} \cap {}^nQ \subseteq \tau^{(\mathcal{B},v)}$, we must have $|\tau^{(\mathcal{B},v)}| \geq r$.
Conversely, suppose that $|\tau^{(\mathcal{A},u)}| < r$. By $(**)$, $\tau^{(\mathcal{A},u)} \subseteq {}^nQ$. Let $t \in \tau^{(\mathcal{B},v)}$ be arbitrary, and let $h \in G$ be such that $th \in {}^nK$. Then by lemma 6, $th \in \tau^{(\mathcal{B},v)}$, so by the inductive hypothesis, $th \in \tau^{(\mathcal{A},u)} \subseteq {}^nQ$. But by definition of G, h fixes Q pointwise, so $th = t$. Thus, $t \in \tau^{(\mathcal{A},u)}$. So $\tau^{(\mathcal{B},v)} \subseteq \tau^{(\mathcal{A},u)}$, giving $|\tau^{(\mathcal{B},v)}| \leq |\tau^{(\mathcal{A},u)}| < r$. This proves the claim.

Now, for all $s \in {}^nK$, $s \in (\mathsf{e}_r\tau)^{(\mathcal{A},u)}$ iff $s \in 1^{\mathcal{A}}$ and $|\tau^{(\mathcal{A},u)}| \geq r$, iff $s \in 1^{\mathcal{B}}$ and $|\tau^{(\mathcal{B},v)}| \geq r$ (by the case $\tau = 1$ and the claim), iff $s \in (\mathsf{e}_r\tau)^{(\mathcal{B},v)}$.

This proves the lemma. ♣

Corollary 8 *$\sigma^{(\mathcal{A},u)} = \tau^{(\mathcal{A},u)}$ iff $\sigma^{(\mathcal{B},v)} = \tau^{(\mathcal{B},v)}$, for all $\sigma, \tau \in \mathcal{T}$.*

Proof.

Assume that $\sigma^{(\mathcal{A},u)} \neq \tau^{(\mathcal{A},u)}$. Let, say, $s \in \tau^{(\mathcal{A},u)} \setminus \sigma^{(\mathcal{A},u)}$. Let $t \in {}^nK$ be such that $\mathfrak{U}(s) \cong \mathfrak{U}(t)$. By lemma 5, $t \in \tau^{(\mathcal{A},u)} \setminus \sigma^{(\mathcal{A},u)}$. As $t \in {}^nK$, by lemma 7 we have $t \in \tau^{(\mathcal{B},v)} \setminus \sigma^{(\mathcal{B},v)}$, so that $\tau^{(\mathcal{B},v)} \neq \sigma^{(\mathcal{B},v)}$.

In the other direction, assume $s \in \tau^{(\mathcal{B},v)} \setminus \sigma^{(\mathcal{B},v)}$. Then $s \in 1^{\mathcal{B}}$ by $s \in \tau^{(\mathcal{B},v)}$, so $sg \in {}^nK$ for some $g \in G$. Then $sg \in \tau^{(\mathcal{B},v)} \setminus \sigma^{(\mathcal{B},v)}$ by lemma 6, and then $sg \in \tau^{(\mathcal{A},u)} \setminus \sigma^{(\mathcal{A},u)}$ by $sg \in {}^nK$ and lemma 7. ♣

This says that $\mathcal{A} \models \sigma = \tau[u]$ iff $\mathcal{B} \models \sigma = \tau[v]$ for all $\sigma, \tau \in \mathcal{T}$, which finishes the proof of the first part of theorem 4.

Finally, we can compute an upper bound $\beta(\phi)$ for the cardinality of the base of $\mathcal{B}$ from our universal sentence ϕ as follows. From ϕ we can compute $\mathcal{T}$, and from $\mathcal{T}$ we can compute an upper bound for $|Q|$. Then from $\mathcal{T}, |Q|$ we can compute an upper bound for the number of isomorphism types of the structures $\mathfrak{U}(s)$. This gives an upper bound for $|K|$, from which Herwig's theorem gives an upper bound for $|K^+|$, which bounds the size of the base of $\mathcal{B}$.

It follows that the universal theory of C is decidable. For, given a universal sentence ϕ of the signature of C, we may compute $\beta(\phi)$ as above, enumerate the finitely many algebras in the reduct of C to the symbols in ϕ with base of size at most $\beta(\phi)$, and evaluate ϕ in each. If we find one in which ϕ is false, then obviously ϕ is not valid in C. If not, then ϕ is valid in C.

It also follows that any reduct to a finite signature (say Σ) of a finite algebra in C is isomorphic in this signature to an algebra in C with finite base. For if $\mathcal{A} \in \mathsf{C}$ is finite, with domain $\{a_0, \ldots, a_{d-1}\}$, say, let $\phi(x_0, \ldots, x_{d-1})$ be a formula representing the diagram of $\mathcal{A}$ in Σ. (So ϕ is the conjunction of all Σ-formulas of the form $x_{i_0} = f(x_{i_1}, \ldots, x_{i_r})$, where $f \in \Sigma$, $\{i_0, \ldots, i_r\} \subseteq d$, and $a_{i_0} = f^{\mathcal{A}}(a_{i_1}, \ldots, a_{i_r})$, together with $\bigwedge_{i<j<d} x_i \neq x_j$.) Then $\forall \bar{x} \neg \phi(\bar{x})$ is not valid in C, as it is not true in $\mathcal{A}$. Hence there is $\mathcal{B} \in \mathsf{C}$ with finite base, and elements $b_0, \ldots, b_{d-1} \in B$ such that $\mathcal{B} \models \phi(\bar{b})$. The map $(a_i \mapsto b_i)_{i<d}$ is then a Σ-embedding : $\mathcal{A} \hookrightarrow \mathcal{B}$, so the restriction of $\mathcal{B}$ to $\{b_0, \ldots, b_{d-1}\}$ is an algebra in C with finite base and isomorphic to $\mathcal{A}$ in signature Σ.

This completes the proof of theorem 4. ♣

3 Corollaries

Now we want to prove the finite base property for more classes of algebras. This is not so hard: quite a few familiar classes can be obtained as *subreduct classes* of C; and we will show (corollary 10) that taking subreducts preserves the finite base property.

3.1 Subreduct classes

First we define what we mean by a subreduct class of C. We can get one by omitting some operations, by making restrictions on the unit of the algebras, and even by adding some new operations.

Definition 9 (A subreduct class of C) Let $\bar{y} = \langle y_0, \ldots, y_{m-1}\rangle$ be a sequence of variables. We will call y_i, $i < m$, parameter variables; other variables will be called non-parameter variables.

Let $\chi = \langle \eta, \tau_1, \ldots, \tau_k\rangle$ be a sequence, where $\tau_1, \ldots, \tau_k$ are terms in the language of C, and $\eta(\bar{y}, x)$ is a quantifier-free formula in the language of C which contains exactly one non-parameter variable (x). The signature associated to χ consists of function symbols $f_1, \ldots, f_k$, where the arity of f_i, $1 \leq i \leq k$, is the number of non-parameter variables of τ_i. Of course, we identify a 0-ary function symbol with a constant.

Assume that for every $\mathcal{A} \in \mathsf{C}$ and every m-tuple $\bar{a}$ of elements (parameters) from $\mathcal{A}$, the set

$$\eta^{\mathcal{A}}(\bar{a}) =_{\text{def.}} \{b \in A : \mathcal{A} \models \eta(\bar{a}, b)\}$$

is closed under the functions on A defined by the $\tau_i^{\mathcal{A}}(\bar{a})$, for each i. Then if $\eta^{\mathcal{A}}(\bar{a})$ is non-empty, we obtain an algebra $\mathcal{A}_{\bar{a}}$ in the new signature $\{f_1, \ldots, f_k\}$. Its domain $A_{\bar{a}}$ is $\eta^{\mathcal{A}}(\bar{a})$, and the function symbols f_i are interpreted in it as the restrictions to $A_{\bar{a}}$ of the functions defined by the $\tau_i^{\mathcal{A}}(\bar{a})$, for each i ($1 \leq i \leq k$).

If $\eta^{\mathcal{A}}(\bar{a})$ is empty, then by convention we let $\mathcal{A}_{\bar{a}}$ be the one-element algebra with doamin $\{\emptyset\}$.

1. We say that an algebra of the signature associated to χ is a *χ-subreduct* of $\mathcal{A} \in \mathsf{C}$ if it is a subalgebra of $\mathcal{A}_{\bar{a}}$ for some $\mathcal{A} \in \mathsf{C}$ and parameters $\bar{a}$ from $\mathcal{A}$.

   Note that its domain is a subset of the domain of $\mathcal{A}$.

2. The χ-subreduct class C_χ of C is defined as the class of all χ-subreducts of algebras in C.

3. A subreduct class of C is a χ-subreduct class for some χ.

COROLLARY 10 *Let C' be a subreduct class of C. Then C' has the finite base property: if a universal sentence fails in C', then it fails in a member of C' with finite base. An upper bound for the size of this finite base can be computed from the universal sentence. Thus, the set of universal formulas valid in C' is decidable.*

PROOF.

Let C' be the χ-subreduct class of C, where $\chi = \langle \eta, \tau_1, \ldots, \tau_k \rangle$. Let $\psi(\bar{x})$ be a quantifier-free formula in the language of C', and assume that $\mathcal{A}' \not\models \forall \bar{x} \psi$ for some $\mathcal{A}' \in \mathsf{C}'$. Let $\mathcal{A} \in \mathsf{C}$, and $\bar{a}$ be an m-tuple of elements of A, such that $\mathcal{A}' = \mathcal{A}_{\bar{a}}$. If $\eta^{\mathcal{A}}(\bar{a})$ is empty, then $\mathcal{A}'$ is the one-element algebra, which is clearly isomorphic to an algebra with base of size 0; so already $\forall \bar{x} \psi$ fails in an algebra with finite base. Assume not. Then

$$\mathcal{A} \models \exists \bar{y} \exists \bar{x} \Bigg(\bigwedge_{1 \le i \le \mathrm{len}(\bar{x})} \eta(\bar{y}, x_i) \wedge \neg \psi' \Bigg),$$

where ψ' is the formula we get from ψ by replacing each function symbol f_i with its 'definition' τ_i (in the obvious way; we do not go into the detailed definition now), and $\bar{y}$ are the parameter variables. By theorem 4, there is $\mathcal{B} \in \mathsf{C}$ with finite base such that

$$\mathcal{B} \models \exists \bar{y} \exists \bar{x} (\bigwedge_i \eta(\bar{y}, x_i) \wedge \neg \psi').$$

Then $\forall \bar{x} \psi$ fails in the biggest χ-subreduct of $\mathcal{B}$, which is in C' and has finite base, a subset of the base of $\mathcal{B}$. Also, by theorem 4, an upper bound on the size of the base of $\mathcal{B}$ can be computed from the formula $\exists \bar{y} \exists \bar{x} (\bigwedge_i \eta(\bar{y}, x_i) \wedge \neg \psi')$, and hence from ψ. Thus, the universal theory of C' is decidable. ♣

3.2 Special cases

In this section we define some special classes of algebras investigated in the literature, and then we will show that they are all subreduct classes of C. Here, n remains the dimension of C.

DEFINITION 11 1. Crs_n is the class of all subalgebras of algebras of the form

$$\langle \wp(W), \cdot, -, 0, 1, \mathsf{c}_i, \mathsf{d}_{ij} \rangle_{i,j<n},$$

where $W \subseteq {}^nU$ for some set U. Recall that we are writing c_i instead of $\mathsf{c}_{(\{i\})}$.

2. Polyadic Crs_n is the class of all subalgebras of algebras of the form

$$\langle \wp(W), \cdot, -, 0, 1, \mathsf{c}_i, \mathsf{s}_{(i,j)}, \mathsf{s}_{[i/j]} \rangle_{i,j<n},$$

where $W \subseteq {}^nU$ for some set U. Here, we write (i,j) for the transposition map $\sigma : n \to n$ given by $\sigma(i) = j$, $\sigma(j) = i$, and $\sigma(k) = k$ for all $k \in n \setminus \{i,j\}$. We write $[i/j]$ for the map $: n \to n$ given by: $[i/j](i) = j$, and $[i/j](k) = k$ for all $k < n$ with $k \neq i$.

3. We obtain C^+ from C by adding the combined substitution-cylindrification operations $\mathsf{s}_{\sigma,\Gamma}$ for all $\sigma : n \to n$ and $\Gamma \subseteq n$. Take an algebra $\mathcal{A}$ in C, let its unit be W, and let $a \in A$. Then

$$\mathsf{s}_{\sigma,\Gamma}(a) = \{s \in W : s \circ \sigma \equiv_\Gamma t \text{ for some } t \in a\}.$$

Note that in the above definition, $s \circ \sigma$ does not necessarily belong to W, and indeed, $\mathsf{s}_{\sigma,\Gamma}$ is not expressible from s_σ and $\mathsf{c}_{(\Gamma)}$ for arbitrary W.

We interpose a lemma on a certain 'reflexivity' restriction on the unit.

LEMMA 12 *Let $\mathcal{A} \in \mathsf{C}$ and let $W = 1^{\mathcal{A}}$ be the unit of $\mathcal{A}$. The following are equivalent.*

1. *$\mathcal{A}$ is* locally cubic [VM] — *i.e., if $s \in W$ and $\sigma : n \to n$ then $s \circ \sigma \in W$*
2. *$\mathcal{A} \models s_\sigma 1 = 1$ for all $\sigma : n \to n$*
3. *W is the union of* Cartesian spaces — *sets of the form ${}^nU$ for some set U.*

PROOF.

$1 \Rightarrow 2$: Assume that $\mathcal{A}$ is locally cubic, and let $\sigma : n \to n$ be given. If $s \in W$ then $s \circ \sigma \in W$, so $s \in (s_\sigma 1)^{\mathcal{A}}$. That is, $W \subseteq (s_\sigma 1)^{\mathcal{A}}$. The converse inclusion is obvious; so $\mathcal{A} \models s_\sigma 1 = 1$.

$2 \Rightarrow 3$: Assume that $\mathcal{A} \models s_\sigma 1 = 1$ for all $\sigma : n \to n$. Let $s \in W$. For any $\sigma : n \to n$, (2) gives $s \in (s_\sigma 1)^{\mathcal{A}}$, so $s \circ \sigma \in W$. We have proved $s \in {}^n\mathrm{Rng}(s) \subseteq W$, from which $W = \bigcup_{s \in W} {}^n Rng(s)$ follows, giving (3).

$3 \Rightarrow 1$: clear. ♣

DEFINITION 11 (CONTINUED) 4. The subclass C^{lc} of C consists of all locally cubic algebras in C.

5. A locally cubic n-dimensional relativized cylindric set algebra augmented with substitution operators is a subalgebra of a locally cubic algebra of the form

$$\langle \wp(W), \cdot, -, 0, 1, \mathsf{c}_i, \mathsf{s}_\sigma, \mathsf{d}_{ij} \rangle_{i,j<n,\, \sigma:n\to n}.$$

   Note that such a subalgebra will itself be locally cubic. We write S_n for the class of all such algebras.

6. The classes G_n, D_n are defined as follows:

$$\mathsf{G}_n = \{\mathcal{A} \in \mathsf{Crs}_n : \mathcal{A} \text{ is locally cubic}\}$$
$$\mathsf{D}_n = \{\mathcal{A} \in \mathsf{Crs}_n : \mathcal{A} \models \mathsf{c}_i \mathsf{d}_{ij} = 1 \text{ for all } i, j < n\}.$$

   We have $\mathsf{G}_n \subseteq \mathsf{D}_n \subseteq \mathsf{Crs}_n$.

The class Crs_n is extensively investigated in the literature, e.g. in [HMTAN, HMT (section 5.5), Monk93, ABN1]. The class S_n is investigated, for example, in [VM], and the classes G_n and D_n in [N86, N96, AGN]. The class C^+ is studied in [N96].

LEMMA 13 *All the classes defined in definition 11 are subreduct classes of* C.

PROOF.

Crs_n and polyadic Crs_n are obtained from C simply by omitting some operations. We can get Crs_n, for example, by taking

$$\begin{array}{lcl} \eta(x) & = & x = x \\ \tau_\cdot(x,z) & = & x \cdot z \\ \tau_-(x) & = & -x \\ \tau_{\mathsf{c}_i}(x) & = & \mathsf{c}_i(x) \quad \text{for all } i < n, \text{ etc.} \end{array}$$

C^+ is obtained from C by adding a new operation $\mathsf{s}_{\sigma,\Gamma}$. C^+ is rendered a χ-subreduct of C by letting

$$\begin{array}{lcl} \eta(y,x) & = & x \leq y \wedge \bigwedge_{\sigma:n\to n} \mathsf{s}_\sigma 1 = 1 \\ \tau_\cdot(x,z) & = & y \cdot (x \cdot z) \\ \tau_-(x) & = & y \cdot -x, \quad \text{etc. (i.e., relativize C-operations to } y) \\ \tau_{\mathsf{s}_{\sigma,\Gamma}}(x) & = & y \cdot \mathsf{s}_\sigma \mathsf{c}_{(\Gamma)}(x). \end{array}$$

Notice that $\eta^{\mathcal{A}}(a)$ is closed under the functions so defined, for all $\mathcal{A} \in \mathsf{C}$ and parameters a from $\mathcal{A}$. If $\mathcal{A} \in \mathsf{C}$ is such that $1^{\mathcal{A}}$ is not closed under all s_σ, then for all $a \in A$, $\eta^{\mathcal{A}}(a)$ is the empty set, giving the one-element algebra as the χ-subreduct of $\mathcal{A}$. Otherwise, by lemma 12 $\mathcal{A}$ is locally cubic, and it follows that the meaning of $\mathsf{s}_{\sigma,\Gamma}$ in χ-subreducts $\mathcal{A}'$ of $\mathcal{A}$ is as intended. It can be checked that all algebras in C^+ arise in this way.

C^{lc} is obtained from C by making a restriction on the unit 1. We can obtain C^{lc} as a χ-subreduct class of C by letting

$$\eta(x) \quad = \quad (x = x) \wedge \bigwedge_{\sigma : n \to n} \mathsf{s}_\sigma 1 = 1.$$

If $\mathcal{A} \in \mathsf{C}$ is not locally cubic then $\eta^{\mathcal{A}}$ is again the empty set, giving the one-element algebra as the χ-subreduct of $\mathcal{A}$. In the other cases, where $\mathcal{A}$ is locally cubic, the χ-subreduct of $\mathcal{A}$ is itself.

S_n, D_n, and G_n are obtained by combining these methods. ♣

COROLLARY 14 *All the classes defined in definition 11 have the finite base property. In particular, a finite algebra in them is representable on a finite set, and the universal theory of the class is the same as that of the finite members. Further, the universal theories of the above classes are decidable.*

PROOF.

Use corollary 10, lemma 13, and also lemma 29 below. ♣

Finally, we note that we can look at theorem 4 as stating a combinatorial principle. Namely, it states that if a 'pattern' is realizable by n-ary relations at all, then it is realizable by finite n-ary relations also. Here by a pattern we mean a finite partial algebra in the similarity type of C. (By a finite partial algebra we mean one with finite domain, and with finitely many operations defined only.)

4 Generalisations

We can prove the finite base property for more classes using a recent strengthening of theorem 1, done by Herwig in [He2]. This gives a structure $\mathfrak{K}^+ \supseteq \mathfrak{K}$ as in theorem 1 that 'looks locally like $\mathfrak{K}$' — roughly, any substructure of $\mathfrak{K}^+$ that is 'packed together', in that any pair of distinct elements of it can be extended to a tuple lying in a relation, can be found already in $\mathfrak{K}$, except that extra relations may hold on the copy in $\mathfrak{K}$. This means that we can handle more operators than were in the class C. We discuss the strengthened theorem first, and then we apply it to algebras. Although theorem 23 and remark 26 below can be adapted to give theorem 4, we think it valuable to present both proofs because the argument in theorem 4 uses a more elementary version of Herwig's theorem.

4.1 Strengthening Herwig's theorem

First, a definition.

DEFINITION 15 Let L be a relational signature, and $\mathfrak{M}, \mathfrak{N}$, L-structures.

1. A tuple $(a_1, \ldots, a_m)$ of elements of M is said to be *live in* $\mathfrak{M}$ if $\mathfrak{M} \models \alpha(a_1, \ldots, a_m)$ for some atomic L-formula $\alpha(x_1, \ldots, x_m)$ in which all of $x_1, \ldots, x_m$ occur.

2. $\mathfrak{M}$ is said to be *irreflexive* if whenever $a_1, \ldots, a_m \in M$, $R \in L$, and $\mathfrak{M} \models R(a_1, \ldots, a_m)$ then the a_i are pairwise distinct.

3. $\mathfrak{M}$ is said to be *packed* if for any $x, y \in M$ there are m-ary $R \in L$ and elements $a_1, \ldots, a_m \in M$ with $x, y \in \{a_1, \ldots, a_m\}$ and $\mathfrak{M} \models R(a_1, \ldots, a_m)$.

4. A map $\nu : M \to N$ is said to be a *weak homomorphism* : $\mathfrak{M} \to \mathfrak{N}$ if whenever $R \in L$ is m-ary, $a_1, \ldots, a_m \in M$, and $\mathfrak{M} \models R(a_1, \ldots, a_m)$, then $\mathfrak{N} \models R(a_1\nu, \ldots, a_m\nu)$.

   Example: (a, a) is always live in $\mathfrak{M}$, as $\mathfrak{M} \models a = a$. Note that ν may not be one to one, and that fewer relations may hold on a tuple in $\mathfrak{M}$ than on its image in $\mathfrak{N}$.

The following can be easily extracted from [He2].

THEOREM 16 (HERWIG) *Let $\mathfrak{K}$ be a finite irreflexive structure in a finite relational signature L. There is a finite irreflexive L-structure $\mathfrak{K}^+ \supseteq \mathfrak{K}$ with the following properties.*

1. *Any partial isomorphism of $\mathfrak{K}$ is induced by an automorphism of $\mathfrak{K}^+$.*

2. *If s is a live tuple in $\mathfrak{K}^+$, then there is $g \in Aut(\mathfrak{K}^+)$ such that sg is a tuple of elements of K.*

3. *For any packed irreflexive L-structure $\mathfrak{M}$, if there is a weak homomorphism $\nu^+ : \mathfrak{M} \to \mathfrak{K}^+$, then there is a weak homomorphism $\nu : \mathfrak{M} \to \mathfrak{K}$.*

There is also a recursive (in $\mathfrak{K}$) upper bound for the size of K^+.

It is easy to show that irreflexivity is not needed here. At the same time, we take the opportunity to put the theorem in the form we will use. For this, we need the following definition.

DEFINITION 17 Let L be a relational signature. A first-order L-formula $\pi(x_1, \ldots, x_m)$ with free variables $x_1, \ldots, x_m$ is said to be *packed* if (a) it is a conjunction of atomic L-formulas, and (b) whenever $1 \leq i < j \leq m$, there is a conjunct of π in which x_i, x_j both occur.

COROLLARY 18 *Let $\mathfrak{K}$ be any finite structure in a finite relational signature L. There is a finite L-structure $\mathfrak{K}^+ \supseteq \mathfrak{K}$ with the following properties.*

1. *Any partial isomorphism of $\mathfrak{K}$ extends to an automorphism of $\mathfrak{K}^+$.*

2. *If s is a live tuple in $\mathfrak{K}^+$, then there is $g \in Aut(\mathfrak{K}^+)$ such that sg is a tuple of elements of K.*

3. *For any packed L-formula $\pi(\bar{x})$, if $\mathfrak{K}^+ \models \exists\bar{x}\pi(\bar{x})$ then $\mathfrak{K} \models \exists\bar{x}\pi(\bar{x})$.*

PROOF (SKETCH).

The idea is very simple: we introduce relations of lower arity that replace the original ones wherever they are reflexive. This makes $\mathfrak{K}$ irreflexive, and we can apply theorem 16. Then we put the original relations back.

In a little more detail, for each n, each n-ary $R \in L$, and each equivalence relation E on n, we introduce a new $|n/E|$-ary relation symbol R_E. Let L' consist of these new symbols. We also choose a transversal T_E for each E: that is, T_E is a set of representatives, one from each E-class on n. And for an n-tuple s, we let E_s be the equivalence relation $\{(i,j) : i,j < n, s_i = s_j\}$ on n.

Define an L'-structure $\mathfrak{K}'$ with domain K as follows. For $R_E \in L'$, we let

$$(R_E)^{\mathfrak{K}'} = \{s\lceil T_{E_s} : s \in R^{\mathfrak{K}}, E_s = E\}.$$

Then $\mathfrak{K}'$ is irreflexive. Let $\mathfrak{K}'^+ \supseteq \mathfrak{K}'$ be as in theorem 16. Define an L-structure $\mathfrak{K}^+$ with domain K'^+ as follows. For $R \in L$, of arity n, say, let

$$R^{\mathfrak{K}^+} = \{s \in {}^nK'^+ : s\lceil T_{E_s} \in (R_{E_s})^{\mathfrak{K}'^+}\}.$$

Note that $Aut(\mathfrak{K}'^+) = Aut(\mathfrak{K}^+)$.

We check that $\mathfrak{K}^+$ fits the bill. Evidently, $\mathfrak{K}$ is a substructure of it. If α is a partial isomorphism of $\mathfrak{K}$, it is also a partial isomorphism of $\mathfrak{K}'$, so it extends to an automorphism g of $\mathfrak{K}'^+$. Then g is an automorphism of $\mathfrak{K}^+$ extending α. Hence (1) holds. For (2), if $|\mathrm{Rng}(s)| = 1$, it is clear. If $\mathfrak{K}^+ \models R(s)$, then $\mathfrak{K}'^+ \models R_{E_s}(s\lceil T_{E_s})$, so $s\lceil T_{E_s}$ is live in $\mathfrak{K}'^+$ and by theorem 16(2) is mapped into K' by some automorphism g of $\mathfrak{K}'^+$. Then g is also an automorphism of $\mathfrak{K}^+$ and maps s into K. So (2) holds.

For (3), let $\pi(x_1, \ldots, x_m)$ be a packed L-formula, let $s \in {}^mK^+$, and suppose that $\mathfrak{K}^+ \models \pi(s)$. Let $\mathfrak{M}$ be the substructure of $\mathfrak{K}'^+$ with domain $\mathrm{Rng}(s)$. If $|\mathrm{Rng}(s)| = 1$, then by (2) above, there is $g \in Aut(\mathfrak{K}^+)$ mapping s into K, so $\mathfrak{K} \models \exists\bar{x}\pi(\bar{x})$. Assume that $|\mathrm{Rng}(s)| > 1$. As $\mathfrak{K}'^+$ is irreflexive, it can be checked that $\mathfrak{M}$ is a packed irreflexive L'-structure. The inclusion map is clearly a weak homomorphism from $\mathfrak{M}$ into $\mathfrak{K}'^+$. Hence, by condition (3) for $\mathfrak{K}'^+$, there exists a weak homomorphism $\nu : \mathfrak{M} \to \mathfrak{K}'$. Note that because $\mathfrak{M}$ is packed and $\mathfrak{K}'$ is irreflexive, ν must be one-to-one. It follows that $\mathfrak{K} \models \pi(s\nu)$. So (3) holds. ♣

4.2 Applications

DEFINITION 19 Let Σ be a functional signature, and let $n \geq 1$.

1. We say that an algebra $\mathcal{A}$ of signature Σ has *dimension* n if there are sets U, W (called the *base* and *unit* of $\mathcal{A}$, respectively) with $A \subseteq \wp(W)$ and $W \subseteq {}^nU$, W, U being as small as possible subject to this.

Clearly, if $\mathcal{A}$ has a dimension then its base and unit are uniquely determined.

2. Let $f \in \Sigma$ be an r-ary function symbol, let $\delta(x_0, \ldots, x_{n-1})$ be a first-order formula of the signature $\{\bar{1}, R_1, \ldots, R_r\}$ (all n-ary relation symbols), and let $\mathcal{A}$ be an n-dimensional algebra of signature Σ with base U and unit W. We say that f is *defined by δ in $\mathcal{A}$,* and that δ is the *table* of f (in $\mathcal{A}$), if

$$f^{\mathcal{A}}(a_1, \ldots, a_r) = \{s \in {}^nU : (U, W, a_1, \ldots, a_r) \models \delta(s)\} \quad \text{for all } a_1, \ldots, a_r \in A,$$

   where in the structure $(U, W, a_1, \ldots, a_r)$, the symbol $\bar{1}$ is interpreted as $W \subseteq {}^nU$, and R_i is interpreted as a_i (where $1 \leq i \leq r$).

3. A table $\delta(\bar{x}, R_1, \ldots, R_r)$ is said to be *existential-packed,* or 'EP', for short, if it is of the form

$$\delta(\bar{x}, R_1, \ldots, R_r) \quad = \quad \mu(\bar{x}) \wedge \exists \bar{y}(\varepsilon(\bar{x}, \bar{y}) \wedge \pi(\bar{y})).$$

   Here:

   - $\bar{x} = x_0, \ldots, x_{n-1}$, $\bar{y} = y_0, \ldots, y_{m-1}$ for some $m < \omega$, and all the x_i, y_j are distinct variables.
   - ε is a (possibly empty) conjunction of equalities of the form $x_i = y_j$, equating elements of $\bar{x}$ with elements of $\bar{y}$.
   - μ and π are quantifier-free formulas of the signature $\{\bar{1}, R_1, \ldots, R_r\}$; they may involve equality, too.
   - $\mu(\bar{x}) \vdash \alpha(\bar{x})$ for some atomic formula $\alpha(\bar{x})$ of signature $\{\bar{1}, R_1, \ldots, R_r\}$ in which all variables in $\bar{x}$ occur free.
   - π is packed.

EXAMPLE 20 All of the operations of definition 2 are EP (i.e., definable by EP tables), except for the counting quantifiers:

- The boolean operations are EP. Their tables are

$$\begin{aligned} \delta_0(\bar{x}) &= x_0 \neq x_0 \\ \delta_1(\bar{x}) &= \bar{1}(\bar{x}) \\ \delta_-(\bar{x}, R) &= \bar{1}(\bar{x}) \wedge \neg R(\bar{x}) \\ \delta_\cdot(\bar{x}, R_1, R_2) &= R_1(\bar{x}) \wedge R_2(\bar{x}). \end{aligned}$$

  Here, '$\exists \bar{y}(\varepsilon(\bar{x}, \bar{y}) \wedge \pi(\bar{y}))$' is the 'empty formula' (i.e., we choose $m = 0$).

- d_{ij} is a nullary function with table $\bar{1}(\bar{x}) \wedge x_i = x_j$.
- For $\sigma : n \to n$, s_σ is a unary function with table $\bar{1}(\bar{x}) \wedge R(x_{\sigma(0)}, \ldots, x_{\sigma(n-1)})$.
- For $\Gamma \subseteq n$, $\mathsf{c}_{(\Gamma)}$ is a unary function with table $\bar{1}(\bar{x}) \wedge \exists y_0 \ldots y_{n-1}((\bigwedge_{i \in n \setminus \Gamma} x_i = y_i) \wedge R(y_0, \ldots, y_{n-1}))$.

Further EP operations are also possible. The simultaneous cylindrification-substitution operations $\mathsf{s}_{\sigma,\Gamma}$ of section 3.2 may be introduced in this way. We may also define, in the manner of Marx and Németi (see [MNS]), an EP product $p(a_0, \ldots, a_{n-1})$ of n n-ary relations, with table of the form

$$\bar{1}(\bar{x}) \wedge \exists y_0 \ldots y_n \Bigg(\bigwedge_{i<n} x_i = y_i \wedge \Bigg[\bigwedge_{i<n} R_i(y_0, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n) \wedge \bar{1}(y_0, \ldots, y_{n-1}) \Bigg] \Bigg).$$

(The final $\bar{1}(y_0, \ldots, y_{n-1})$ is needed when $n = 2$, to make the 'π'-part packed, although omitting it does not change the logical meaning of the table.) Modulo a minor permutation of variables, in the case $n = 2$ this yields the classical product of two binary relations, relativized to the unit. The classical converse $\breve{a}$ of a binary relation a is also EP. See example 22 below.

A final typical example comes from [J], in which the following m^2-ary operation on binary relations is defined and investigated: the defining formula is

$$Q_m(x_0, x_1, \langle R_{ij} : i, j < m \rangle) = \exists y_0 \ldots y_{m-1}(x_0 = y_0 \wedge x_1 = y_{m-1} \wedge \bigwedge_{i,j<m} R_{ij}(y_i, y_j)).$$

This is an EP formula.

Definition 21 Let Σ be a a functional signature. A class K of algebras of signature Σ is said to be EP if there are a number $n \geq 1$, an EP table δ_f associated to each $f \in \Sigma$, and an existential sentence ξ of the signature Σ, such that K is the class of all n-dimensional algebras $\mathcal{A}$ of signature Σ such that (i) each $f \in \Sigma$ is defined in $\mathcal{A}$ by δ_f, and (ii) $\mathcal{A} \models \xi$.

Example 22 The class WA of *weakly associative algebras,* defined in [Madd], is the closure under isomorphism of an EP class. For it may be defined as the isomorphism-closure of the class of all two-dimensional algebras of signature $\Sigma = \{\cdot, -, 0, 1, Id, \smile, ;\}$ (Id is nullary, $\smile$ unary, and ; binary), where the defining sentence ξ is $(1 = \breve{1}) \wedge (1 = Id; 1)$ (which is quantifier-free), and the tables are as follows:

- For the boolean functions $\cdot, -, 0, 1$ see example 20.
- $\delta_{Id}(x_0, x_1) \quad = \quad x_0 = x_1$
- $\delta_{\smile}(x_0, x_1, R) \quad = \quad R(x_1, x_0)$
- $\delta_{;}(x_0, x_1, R_1, R_2) =$
  $\bar{1}(x_0, x_1) \wedge \exists y_0 y_1 y_2(x_0 = y_0 \wedge x_1 = y_1 \wedge R_1(y_0, y_2) \wedge R_2(y_2, y_1) \wedge \bar{1}(y_0, y_1))$

(As before, the final $\bar{1}(y_0, y_1)$ is there to ensure packedness; its omission does not change the meaning.) The sentence ξ enforces that the unit is a reflexive and symmetric binary relation on the base. The tables enforce that Id is interpreted in WA as equality, $\smile$ as converse, and ; as relation composition, all relativized to the unit. There are related classes in which one or both of the reflexive and symmetric restrictions on the unit are dropped, and these are also EP.

THEOREM 23 *Let $n \geq 1$ be finite, and let* K *be an EP class of n-dimensional algebras. Any universal sentence that is not valid in* K *is falsifiable in an algebra in* K *with finite base. An upper bound for the size of this finite base is computable from the sentence.* K *has decidable universal theory. If the signature of* K *is finite, then any finite algebra in* K *is isomorphic to an algebra in* K *with finite base.*

PROOF.

The proof is much as in theorem 4, and we only mention the differences. We wish to show that any existential sentence $\phi = \exists \bar{z}\psi$ satisfiable in K is in fact satisfiable in some algebra in K with finite base. We may assume that ϕ logically entails the existential sentence ξ that defines K (as in definition 21). Let $\mathcal{T}$ be a finite set of terms that contains all the terms occurring in ψ and is closed under subterms. Assume we are given an algebra $\mathcal{A} \in \mathsf{K}$, and an assignment u of the variables in $\mathcal{T}$ to elements of A, such that $(\mathcal{A}, u) \models \psi$. We will find an n-dimensional algebra $\mathcal{B}$ with finite base of size effectively computable from $\mathcal{T}$, and an assignment v of the variables in $\mathcal{T}$ to elements of B, such that $(\mathcal{B}, v) \models \psi$. Hence, $\mathcal{B} \models \phi$; and as $\phi \vdash \xi$, it follows that $\mathcal{B} \in \mathsf{K}$.

Let U be the base of $\mathcal{A}$. We form a finite relational signature, and a structure $\mathfrak{U}$ with domain U, as follows. First, we introduce an n-ary relation symbol $\overline{1}$ and interpret it in $\mathfrak{U}$ as the unit of $\mathcal{A}$. Then, for each $\tau \in \mathcal{T}$ we introduce an n-ary relation symbol $\overline{\tau}$, and interpret it in $\mathfrak{U}$ as $\tau^{(\mathcal{A},u)}$. But there are more operation symbols. Let $\tau = f(\tau_1, \ldots, \tau_r) \in \mathcal{T}$, where f is an operation defined on the algebras in K by the EP table $\delta = \mu(\bar{x}) \wedge \exists \bar{y}(\varepsilon(\bar{x}, \bar{y}) \wedge \pi(\bar{y}))$. Let $\mu(\bar{x}, \overline{\tau_1}, \ldots, \overline{\tau_r})$ be the result of substituting the relation symbol $\overline{\tau_i}$ for R_i in μ, for each i. Suppose that ε is $\bigwedge_{l<k} x_{i_l} = y_{j_l}$, where $i_0 \leq \cdots \leq i_{k-1} < n$. Then a k-ary relation symbol $\tau\dagger$ is also introduced, and interpreted in $\mathfrak{U}$ as

$$(\tau\dagger)^{\mathfrak{U}} \quad = \quad \{(s_{i_0}, \ldots, s_{i_{k-1}}) : s \in {}^nU \setminus \tau^{(\mathcal{A},u)}, \mathfrak{U} \models \mu(s, \overline{\tau_1}, \ldots, \overline{\tau_r})\}.$$

In the case $\tau = \mathsf{c}_{(\Gamma)}\tau'$, for example, $\tau\dagger^{\mathfrak{U}} = \{s\lceil n \setminus \Gamma : s \in (-\tau)^{(\mathcal{A},u)}\}$.

Choose $\ell \geq n$ such that the table of any operation occurring in $\mathcal{T}$ contains at most ℓ variables, and take a finite substructure $\mathfrak{K} \subseteq \mathfrak{U}$ containing isomorphic representatives of each substructure of $\mathfrak{U}$ of size at most ℓ. Let $\mathfrak{K}^+ \supseteq \mathfrak{K}$ be as in corollary 18. Let $\mathcal{B}$ be the algebra with domain $B = \wp(\overline{1}^{\mathfrak{K}^+})$, the operations being defined by the same tables as they are in K. Certainly, the base of $\mathcal{B}$ is finite — in fact, we have:

LEMMA 24 *The base of $\mathcal{B}$ is K^+, and the unit of $\mathcal{B}$ is $\overline{1}^{\mathfrak{K}^+}$.*

PROOF.

It is clear that $\mathcal{B}$'s unit is $\overline{1}^{\mathfrak{K}^+}$. To show that K^+ is its base, it suffices to take arbitrary $a \in K^+$ and find $s \in \overline{1}^{\mathfrak{K}^+}$ with $a \in \mathrm{Rng}(s)$.

As (a, a) is a live tuple in $\mathfrak{K}^+$ (see definition 15), by corollary 18(2) there is $g \in Aut(\mathfrak{K}^+)$ with $ag \in K$. So we can assume that $a \in K$. As a is (now) in the base U of $\mathcal{A}$, there is $t \in \overline{1}^{\mathfrak{U}}$ with $a \in \text{Rng}(t)$. By choice of K, there is $t' \in \overline{1}^{\mathfrak{K}}$ with $\mathfrak{K}\lceil\text{Rng}(t') \cong \mathfrak{U}\lceil\text{Rng}(t)$. Let $i < n$ be such that $t_i = a$. Then $\{(t'_i, t_i)\}$ is a partial isomorphism of $\mathfrak{K}$ which extends by corollary 18(1) to an automorphism g of $\mathfrak{K}^+$. Let $s = t'g$. Then we see that $a = s_i \in \text{Rng}(s)$ and $s \in \overline{1}^{\mathfrak{K}^+}$. ♣

Define an assignment v of the variables in $\mathcal{T}$ into B by $v(z) = \overline{z}^{\mathfrak{K}^+}$. We can now prove an analogue of lemma 7:

LEMMA 25 *For each term $\tau \in \mathcal{T}$, we have $\tau^{(\mathcal{B},v)} = \overline{\tau}^{\mathfrak{K}^+}$.*

PROOF.

By induction on τ. If τ is a variable then the statement holds by definition of v. Let $\tau = f(\tau_1, \ldots, \tau_r) \in \mathcal{T}$ and assume the result for $\tau_1, \ldots, \tau_r$. For each i we have

$$\tau_i^{(\mathcal{A},u)} = \overline{\tau_i}^{\mathfrak{U}} \quad \text{and} \quad \tau_i^{(\mathcal{B},v)} = \overline{\tau_i}^{\mathfrak{K}^+} \tag{1}$$

(the first by definition of $\mathfrak{U}$, the second by the inductive hypothesis). Let the EP table of f be $\delta(\bar{x}, R_1, \ldots, R_r)$. Substitute the relation symbol $\overline{\tau_i}$ for R_i in this, for each i, to give the formula

$$\delta(\bar{x}) = \mu(\bar{x}) \wedge \exists \bar{y}(\varepsilon(\bar{x}, \bar{y}) \wedge \pi(\bar{y})). \tag{2}$$

We stress that δ, μ, π in (2) will in general involve n-ary predicates from $\{\overline{1}, \overline{\tau_1}, \ldots, \overline{\tau_r}\}$, though for brevity we do not show these explicitly. Then by (1), using lemma 24 for the second line,

$$\begin{array}{lll} \forall s \in {}^nU, & s \in \tau^{(\mathcal{A},u)} & \iff \mathfrak{U} \models \delta(s), \\ \forall s \in {}^nK^+, & s \in \tau^{(\mathcal{B},v)} & \iff \mathfrak{K}^+ \models \delta(s). \end{array} \tag{3}$$

Now we prove the lemma for τ. By (3), it suffices to show that if $s \in {}^nK^+$ then

$$\mathfrak{K}^+ \models \delta(s) \leftrightarrow \overline{\tau}(s). \tag{4}$$

Now if s is a counterexample then s is live in $\mathfrak{K}^+$. ('Live' is defined in definition 15. If $\mathfrak{K}^+ \models \overline{\tau}(s)$ then it is obviously live; and if $\mathfrak{K}^+ \models \delta(s)$ then $\mathfrak{K}^+ \models \mu(s)$, so by the assumption on μ in definition 19(3), $\mathfrak{K}^+ \models \alpha(s)$ for some atomic formula $\alpha(\bar{x})$ of the signature $\{\overline{1}, \overline{\tau_1}, \ldots, \overline{\tau_r}\}$ in which all variables in $\bar{x}$ occur.) So by corollary 18(2), s is mapped into ${}^nK$ by an automorphism of $\mathfrak{K}^+$, and as this automorphism preserves both sides of (4), we see that there is a counterexample to (4) in K.

So we may assume that $s \in {}^nK$.

Suppose first that $\mathfrak{K}^+ \models \overline{\tau}(s)$. Since $s \in {}^nK$ now, we have $\mathfrak{U} \models \overline{\tau}(s)$, and so by definition of $\mathfrak{U}$, $s \in \tau^{(\mathcal{A},u)}$. Let $\bar{y}$ in (2) be $y_0, \ldots, y_{m-1}$, and using (3) let $t \in {}^mU$ be such that $\mathfrak{U} \models \mu(s) \wedge \varepsilon(s,t) \wedge \pi(t)$. There are $s' \in {}^nK$ and $t' \in {}^mK$ such that, as substructures of $\mathfrak{U}$, we have $s't' \cong st$. Then $\mathfrak{K}^+ \models \varepsilon(s',t') \wedge \pi(t')$, as this formula is quantifier-free. Moreover, the map $s' \mapsto s$ is a partial isomorphism of $\mathfrak{K}$. Using corollary 18(1), let $g \in Aut(\mathfrak{K}^+)$ extend it. Then $\mathfrak{K}^+ \models \varepsilon(s, t'g) \wedge \pi(t'g)$. Since $\mathfrak{U} \models \mu(s)$, and this formula is quantifier-free, $\mathfrak{K}^+ \models \mu(s)$, proving that $\mathfrak{K}^+ \models \delta(s)$ as required.

Conversely, if $\mathfrak{K}^+ \models \delta(s)$ then there is $t \in {}^mK^+$ such that $\mathfrak{K}^+ \models \mu(s) \wedge \varepsilon(s,t) \wedge \pi(t)$. Let $\varepsilon = \bigwedge_{l<k} x_{i_l} = y_{j_l}$, where $i_0 \leq \cdots \leq i_{k-1} < n$ and $j_0, \ldots, j_{k-1} < m$. Let

$$\pi^*(\bar{y}) \quad = \quad \pi(\bar{y}) \wedge \tau\dagger(y_{j_0}, \ldots, y_{j_{k-1}}). \tag{5}$$

Claim. $\mathfrak{K}^+ \not\models \pi^*(t)$.

Proof of claim. Assume the contrary. Now π^* is clearly packed, so by corollary 18(3) we have $\mathfrak{K} \models \pi^*(t')$ for some $t' \in {}^mK$. As π^* is quantifier-free, $\mathfrak{U} \models \pi^*(t')$. In particular, $\mathfrak{U} \models \tau\dagger(t'_{j_0}, \ldots, t'_{j_{k-1}})$. By definition of $\tau\dagger^{\mathfrak{U}}$, we may choose $s' \in {}^nU \setminus \tau^{(\mathcal{A},u)}$ with $\mathfrak{U} \models \mu(s)$ and $(s'_{i_0}, \ldots, s'_{i_{k-1}}) = (t'_{j_0}, \ldots, t'_{j_{k-1}})$. But now, $\mathfrak{U} \models \varepsilon(s',t') \wedge \pi(t')$, so $\mathfrak{U} \models \delta(s')$ and (by (3)) $s' \in \tau^{(\mathcal{A},u)}$, a contradiction. This proves the claim.

But we have $\mathfrak{K}^+ \models \pi(t)$, so by the claim, $\mathfrak{K}^+ \not\models \tau\dagger(t_{j_0}, \ldots, t_{j_{k-1}})$. As $\mathfrak{K}^+ \models \varepsilon(s,t)$, this says that $\mathfrak{K}^+ \not\models \tau\dagger(s_{i_0}, \ldots, s_{i_{k-1}})$. But $s \in {}^nU$, so also, $\mathfrak{U} \not\models \tau\dagger(s_{i_0}, \ldots, s_{i_{k-1}})$. As $\mathfrak{K}^+ \models \mu(s)$, the same holds in $\mathfrak{U}$. So by definition of $(\tau\dagger)^{\mathfrak{U}}$ we obtain $s \in \tau^{(\mathcal{A},u)}$. By definition of $\overline{\tau}^{\mathfrak{U}}$, $\mathfrak{U} \models \overline{\tau}(s)$, and as $s \in {}^nK$ we have $\mathfrak{K}^+ \models \overline{\tau}(s)$ as required. The proof of (4) is complete. ♣

It now follows that two terms $\sigma, \tau \in \mathcal{T}$ are equal in $(\mathcal{A}, u)$ iff they are in $(\mathcal{B}, v)$. For if $s \in \sigma^{(\mathcal{A},u)} \setminus \tau^{(\mathcal{A},u)}$ then $\mathfrak{U} \models (\overline{\sigma} \wedge \neg\overline{\tau})(s)$. By choice of K, there is $s' \in {}^nK$ with the same property. By the lemma, $s' \in \sigma^{(\mathcal{B},v)} \setminus \tau^{(\mathcal{B},v)}$. Conversely, if $s \in \sigma^{(\mathcal{B},v)} \setminus \tau^{(\mathcal{B},v)}$ then the lemma yields $\mathfrak{K}^+ \models (\overline{\sigma} \wedge \neg\overline{\tau})(s)$. Hence s is live in $\mathfrak{K}^+$, and by corollary 18(2) we may suppose without loss of generality that $s \in {}^nK$. So $\mathfrak{U} \models (\overline{\sigma} \wedge \neg\overline{\tau})(s)$, giving $s \in \sigma^{(\mathcal{A},u)} \setminus \tau^{(\mathcal{A},u)}$.

It clearly follows that $(\mathcal{B}, v) \models \psi$; so as we said, $\mathcal{B} \models \phi$, $\mathcal{B} \models \xi$, and $\mathcal{B} \in \mathsf{K}$. The rest of the proof is as in theorem 4. ♣

Remark 26 Recall that theorem 4 contained some additional arguments (borrowed from [MM]) to handle the counting quantifiers. These can be included in theorem 23, too, but for simplicity we omitted them. The same idea gives the following. Let K be as in the theorem. Take any finite set $\mathcal{T}$ of terms in the language of K, any $\mathcal{A} \in \mathsf{K}$, and any assignment u of the variables occurring in $\mathcal{T}$ to elements of A. Then there are $\mathcal{B} \in \mathsf{K}$ with finite base and an assignment v of the variables to elements of B such that for all $\tau, \sigma \in \mathcal{T}$:

1. $\mathcal{A} \models (\tau = \sigma)[u]$ iff $\mathcal{B} \models (\tau = \sigma)[v]$.
2. If $\tau^{(\mathcal{A},u)}$ is finite, then $\tau^{(\mathcal{A},u)} = \tau^{(\mathcal{B},v)}$.

However, the proof does not give an effective bound on the size of the base of $\mathcal{B}$ in terms of $\mathcal{T}$.

We indicate the modifications to the proof required to obtain this. We can assume that $\mathcal{T}$ is closed under taking subterms. For any $\tau \in \mathcal{T}$ such that $\tau^{(\mathcal{A},u)}$ is finite, choose a finite subset Q_τ of U such that $\tau^{(\mathcal{A},u)} \subseteq {}^n(Q_\tau)$; otherwise let $Q_\tau = \emptyset$. Set $Q = \bigcup\{Q_\tau : \tau \in \mathcal{T}\} \subseteq U$. Then Q is finite. Include in the signature of $\mathfrak{U}$ additional constant symbols to denote the elements of Q.

Note that any substructure of $\mathfrak{U}$ contains Q. Corollary 18 can be adapted in the style of theorem 4 to signatures with finitely many constant symbols, and lemma 25 can still be proved.

To show $\tau^{(\mathcal{A},u)} = \tau^{(\mathcal{B},v)}$ when the former is finite, assume it is, and let $s \in \tau^{(\mathcal{A},u)}$. Then $s \in {}^nQ \subseteq {}^nK$, so $\mathfrak{K}^+ \models \overline{\tau}[s]$ since $\mathfrak{U} \models \overline{\tau}[s]$, hence $s \in \tau^{(\mathcal{B},v)}$ by lemma 25. Conversely, assume $s \in \tau^{(\mathcal{B},v)}$, i.e., $\mathfrak{K}^+ \models \overline{\tau}[s]$. Then s is live in $\mathfrak{K}^+$, so $s = s'g$ for some $s' \in {}^nK$ and automorphism g of $\mathfrak{K}^+$. Then $\mathfrak{K}^+ \models \overline{\tau}[s']$, hence $\mathfrak{U} \models \overline{\tau}[s']$, i.e., $s' \in \tau^{(\mathcal{A},u)}$, and hence $s' \in {}^nQ$. But each automorphism of $\mathfrak{K}^+$ is the identity on Q, so $s = s'$ and $s \in \tau^{(\mathcal{A},u)}$.

Notice that we obtain as a special case of theorem 23:

COROLLARY 27 *The class* WA *of weakly associative algebras is the closure under isomorphism of a class with the properties cited in theorem 23. The same holds for the related classes in which the unit is not required to be reflexive/symmetric.*

PROOF.

Example 22 shows that WA is the isomorphism-closure of an EP class, so that theorem 23 applies. ♣

5 Discussion

In this section we investigate the notion of finite base property a little more, and then we explore the possible improvements of our theorem 4. The class C is as in definition 2.

DEFINITION 28 1. Let $\mathsf{K} \subseteq \mathsf{C}$, or more generally, $\mathsf{K} \subseteq \mathsf{C}'$ for some subreduct class C' of C. Let $\mathcal{S}$ be a set of sentences. We say that K has the finite algebra property (respectively, finite base property) with respect to $\mathcal{S}$ if whenever a sentence in $\mathcal{S}$ fails in some algebra in K, it also fails in a finite algebra (respectively, in an algebra with finite base) in K.

Thus, K has the finite algebra property of the introduction if it has the finite algebra property with respect to the set of all universal sentences; and similarly for the finite base property.

2. We say that K has the *finite algebra on finite base property* if each finite member of K can be represented on a finite base (i.e., is isomorphic to an algebra in K with finite base).

In other words, K has the finite algebra property with respect to $\mathcal{S}$ means that the $\mathcal{S}$-theory of K is the same as the $\mathcal{S}$-theory of the class of all finite members of K.

We state the following simple lemma without proof.

LEMMA 29 *Let $\mathsf{K} \subseteq \mathsf{C}$, possibly with some C-operations dropped. The following are with respect to arbitrary $\mathcal{S}$.*

1. *Suppose that the similarity type of K is finite. If K has both the finite algebra property and the finite algebra on finite base property then it has the finite base property. The converse holds if $\mathcal{S}$ contains all universal sentences.*

2. *K has the finite algebra (respectively, base) property iff every reduct of an algebra in K to a finite signature Σ is isomorphic to a reduct (to Σ) of a finite algebra (respectively, of an algebra with finite base) in K.*

Using the terminology of definition 28, our theorem 4, corollary 14, and theorem 23 state that the classes $\mathsf{C}, \mathsf{C}^{lc}, \mathsf{Crs}_n$, polyadic Crs_n, etc., all have the finite base property with respect to universal sentences. We now begin to discuss the possible improvements of these statements.

1. Let $\mathsf{Cs}_n = \{\mathcal{A} \in \mathsf{Crs}_n : 1^{\mathcal{A}}$ is a Cartesian space$\}$, and $\mathsf{Gs}_n = \{\mathcal{A} \in \mathsf{Crs}_n : 1^{\mathcal{A}}$ is a disjoint union of Cartesian spaces$\}$. Then $\mathsf{Cs}_2, \mathsf{Gs}_2$ have the finite base property by [HMT, 4.2.8, 3.2.66], while for $n \geq 3$, Cs_n has neither the finite algebra property with respect to equations, nor the finite algebra on finite base property. The same holds for Gs_n, cf. [N84] and [Monk91, status of Problem 4.15].

2. Crs_n for $n \geq 2$ does not have the finite algebra property with respect to existential sentences. This follows from work of Mikulás [Mi], in which an equation e with free variable x is given such that $\mathcal{A} \models e$ for some $\mathcal{A} \in \mathsf{Crs}_n$ while for all $\mathcal{A} \in \mathsf{Crs}_n$, $\mathcal{A} \models e$ implies that $\mathcal{A}$ is infinite. That is, the existential sentence $\exists x \neg e$ fails in Crs_n and it can fail only in infinite algebras in Crs_n. Roughly, the idea in [Mi] is to express with $\forall x\, e$ that the unit 'contains' an injective but non-surjective function on (part of) the base.

3. Here we briefly summarize what is known about the finite base property in the theory of relation algebras. Let RA, SA, WA, Rs respectively denote the classes of all relation algebras, semi-associative relation algebras, weakly associative relation algebras, and

set algebras. For definitions see [HMT, chapter 5.3] and [Madd], for example. Now, RA, SA, Rs do not have the finite algebra property for equations. Rs does not have the finite algebra on finite base property. The proofs for these are adaptations of the ones for the cylindric cases. It is proved in [N87] that WA has the finite algebra property. We proved above (corollary 27) that WA has the finite algebra on finite base property. (This was stated in [N96], but the proof therein contains an error.)

4. It is a useful general question to characterise the operators for which the finite base property holds — that is, what kind of tables, as in definition 19, are allowed?

   First, one might consider adding to the signature of C some more interesting counting quantifiers, of the form e^r_Γ for arbitrary $\Gamma \subseteq n$, with semantics

   $$\mathsf{e}^r_\Gamma a = \{s \in 1^{\mathcal{A}} : |\{t \in a : t \equiv_\Gamma s\}| \geq r\}$$

   for an algebra $\mathcal{A}$ and $a \in A$. However, Mikulás proved in [Mi] that the resulting class does not have the finite algebra property with respect to equations, and indeed, for $n \geq 3$ it has undecidable equational theory. But it still can have, in principle, the finite algebra on finite base property. It would be interesting to know whether it does or not.

5. The preceding point shows that we cannot be too liberal with what operators we include in the signature of C. On the other hand, we can be slightly more general and add any unary operators of the form f_ψ, where $\psi(\bar{y}_0, \ldots, \bar{y}_{r-1})$ may be any quantifier-free first-order formula written with equality only, and $\bar{y}_0, \ldots, \bar{y}_{r-1}$ are n-tuples of distinct variables. The table $\delta(\bar{x}, R)$ of the function f_ψ is

   $$\exists \bar{y}_0 \ldots \bar{y}_{r-1}(\psi(\bar{y}_0, \ldots, \bar{y}_{r-1}) \wedge \bigwedge_{i<r} R(\bar{y}_i)).$$

   See definition 19. As $\bar{x}$ does not occur in δ, the value of f_ψ is always empty or the unit. *It is required of ψ that in any algebra, if a is infinite then $f_\psi a$ is the unit.* We can then adapt the proof of lemma 7, in particular, to handle these operators. The set Q should be chosen so that for each $f_\psi \tau \in \mathcal{T}$, ${}^nQ$ contains some $s_0, \ldots, s_{r-1}$ in $\tau^{(\mathcal{A},u)}$ such that $U \models \psi(s_0, \ldots, s_{r-1})$, if there are any (i.e., if $(\mathcal{A}, u) \models f_\psi \tau = 1$), and the whole of $\tau^{(\mathcal{A},u)}$, if not. Thus, the finite base property still holds.

   Here are some examples of such ψ. (We write y_{ij} for the jth variable in the tuple $\bar{y}_i$.)

   - $\bigwedge_{i<j<r} \bigvee_{k<n} y_{ik} \neq y_{jk}$, for which $f_\psi a = \mathsf{e}_r a$, for all a. The counting quantifiers are therefore expressible by the operators f_ψ.
   - $\bigvee_{\eta: r \to n} \bigwedge_{i<j<r} y_{i,\eta(i)} \neq y_{j,\eta(j)}$, for which $f_\psi a = 1$ says that the 'base' of a, defined in the obvious way, has at least r elements.

   Notice in each case that if a is infinite then there are $s_0, \ldots, s_{r-1} \in a$ such that $U \models \psi(s_0, \ldots, s_{r-1})$, as required. A non-example is

- $\bigwedge_{i<j<r,\, k,l<n} y_{ik} \neq y_{jl}$, for which $f_\psi a = W$ expresses that the argument a has at least r pairwise disjoint sequences.

Here, a may be infinite and yet all its sequences may intersect. We wonder whether adding such an operator destroys the finite base property.

References

ABN1 H. Andréka, J. van Benthem, I. Németi. Modal languages and bounded fragments of predicate logic. J. Philosophical Logic, to appear.

ABN2 H. Andréka, J. van Benthem, I. Németi. Finite model property of bounded fragment of first-order logic and cylindric-relativized set algebras. Budapest, 1995, manuscript.

AGN H. Andréka, R. Goldblatt, I. Németi. Relativised quantification: some canonical varieties of sequence-set algebras. J. Symbolic Logic, to appear.

HMT L. Henkin, J. D. Monk, A. Tarski. Cylindric Algebras, Part I (1971), Part II (1985). North-Holland.

HMTAN L. Henkin, J. D. Monk, A. Tarski, H. Andréka, I. Németi. Cylindric set algebras. Lecture Notes in Mathematics Vol. 883, Springer–Verlag, Berlin, 1981.

He1 B. Herwig. Extending partial isomorphisms on finite structures. Combinatorica 15 (1995) 365–371.

He2 B. Herwig. Extending partial isomorphisms for the small index property of many ω–categorical structures. Israel J. Math., 1996, submitted.

HHMMR R. Hirsch, I. Hodkinson, M. Marx, S. Mikulás, M. Reynolds. Mosaics and step-by-step. Studia Logica, 1996, submitted.

Hr E. Hrushovski. Extending partial isomorphisms of graphs. Combinatorica 12 (1992) 411–416.

J B. Jónsson The theory of binary relations. In: Algebraic Logic (Proc. Conf. Budapest, 1988) Colloq. Math. Soc. J. Bolyai Vol. 54, North-Holland, Amsterdam, 1991. pp. 245–292.

Madd R. Maddux. Some varieties containing relation algebras. Trans. Amer. Math. Soc. 272 (2), 1982, 501–526.

MM M. Marx, S. Mikulás. Decidability and complexity of classical Cs_2. Imperial College, London, 1996, in preparation.

MNS M. Marx, I. Németi, I. Sain. Conjugated Boolean algebras with operators. Manuscript, in preparation.

Mi S. Mikulás. A note on expressing infinity in cylindric-relativized set algebras. King's College London, preprint, 1996.

Monk91 J. D. Monk. Remarks on the problems in the books Cylindric Algebras, Part I and Part II and Cylindric Set Algebras. In: Algebraic Logic, Coll. Soc. J. Bolyai Vol. 54, North-Holland, Amsterdam, 1991. pp.719–722.

Monk93 J. D. Monk. Lectures on cylindric set algebras. In: Algebraic Methods in Logic and in Computer Science (Proc. Banach Semester, Fall 1991, ed. C. Rauszer). Banach Center Publications Vol. 28, Institute of Mathematics, Polish Academy of Sciences, Warsaw 1993, pp. 253–290.

N84 I. Németi. Neither the variety of cylindric algebras nor the variety of representable cylindric algebras is generated by its finite members for dimensions greater than 2. Preprint, Mathematical Institute, Budapest, 1984.

N86 I. Németi. Free algebras and decidability in algebraic logic. Doctoral Dissertation with the Academy, Budapest, 1986.

N87 I. Németi. Decidability of relation algebras with weakened associativity. Proc. Amer. Math. Soc. 100 no. 2 (1987) 340–344.

N92 I. Németi. Decidable versions of first-order logic. In: Logic Colloquium '92, ed. L. Csirmaz, D. Gabbay, M. de Rijke, CSLI Publications & FoLLI, 1995, pp. 177–241.

N96 I. Németi. Fine structure analysis of first order logic. In: Arrow Logic and Multi-Modal Logic, M. Marx, L. Pólos and M. Masuch (eds.), CSLI Publications, 1996, pp. 221–247.

S A. Simon. Nonrepresentable algebras of relations. PhD Dissertation, in preparation. Budapest, 1996.

VM Y. Venema, M. Marx. A Modal Logic of Relations. Studia Logica, to appear (Report no. IR-396, Faculteit der Wiskunde en Informatica, Vrije Universiteit Amsterdam, 1995).

Andréka, Németi:
Mathematical Institute of
Hungarian Academy of Sciences
Pf. 127
1364 Budapest
Hungary

Hodkinson:
Department of Computing
Imperial College
180 Queen's Gate
London SW7 2BZ
UK